Guidance: Privacy and Working from Home

Right to Information and Protection of Privacy Act
Personal Health Information Privacy and Access Act

The purpose of this document is to provide guidance to public bodies under the *Right to Information and Protection of Privacy Act* and health care custodians under the *Personal Health Information Privacy and Access Act*, as well as their employees, to ensure that personal information and personal health information is appropriately protected at all times when working off-site or from home.

In light of the COVID-19 pandemic, many public bodies and health care custodians have significantly altered their day-to-day operations and many employees are now working from home. This guidance document sets out steps employers and employees can take to protect personal information and/or personal health information where employees are asked to or are required to work off-site or from home.

General principles

Despite the significant change in many employees' work situations recently, obligations with respect to the handling of personal information and personal health information continue at all times.

Employees can only collect, use, and/or disclose personal information or personal health information as authorized by law.

The personal information or personal health information involved in a particular task should be limited to the minimum amount necessary to accomplish the purpose and should only be shared with or made accessible to those who need to know it in the course of their work duties.

Steps for employers

- Ensure that you have appropriate policies, practices, and guidelines in place with respect to the protection of personal information and/or personal health information, including directives on retention and processes for secure disposal, and that employees are aware of and have ready access to them.
- Ensure that employees only have access to the personal information and/or personal health information that they need to accomplish their work-related tasks.
- Ensure that employees are advised of the applications, platforms, and systems that have been approved for handling personal information and/or personal health information, including for virtual meetings and online video conferencing.
- Ensure that mobile devices to be used by employees in handling personal information and/or personal health information are as secure as possible:
    - Install password protection and encryption on mobile devices.
    - Consider implementing remote tracking and remote wiping of information on mobile devices, in the event that these are lost or stolen.

    - Consider allowing access to personal information and/or personal health information remotely through virtual private networks and secure servers, rather than having employees store this kind of information remotely on mobile devices.
- Implement a sign-out process for mobile devices and paper records to keep track of which employees have these items.
- Ensure all employees are advised of and are aware of what to do should a privacy or security breach occur, as well as who they are to contact for assistance or to report a potential or actual breach.

Steps for employees

- Consult and follow your employer's policies, practices, guidelines on the handling of personal information and/or personal health information.
- Only use mobile devices, accounts, platforms, and/or networks provided by or approved by your employer for work-related purposes.
    - Consult with your employer about the use of personal devices when working from home.
- Secure paper records during transport and storage at home:
    - Never leave mobile devices or paper records unattended, including in your vehicle, to minimize the risk of unauthorized access, loss, or theft.
- When setting up your workspace at home:
    - Choose an area with as much privacy as possible.
    - Ensure others cannot see or otherwise access personal information or personal health information on paper records or your work devices.
    - Ensure others cannot overhear conversations in which personal information or personal health information is discussed.
    - Only use means approved by your employer to share and store personal information and personal health information:
        - Avoid using non-approved platforms, applications, or networks when handling personal information or personal health information, such as personal email accounts.
        - Do not store personal information or personal health information on devices that are not password-protected and/or encrypted.
    - Ensure mobile devices are locked or shut down when not in use.
    - Ensure mobile devices and paper records are securely stored when not in use, such as in a locked filing cabinet or in a designated area that only the employee can access.
    - Do not allow others to use mobile devices that are used for work purposes.
    - Do not share passwords to mobile devices that are used for work purposes.
- Be wary of phishing attempts or potential fraudulent activities that may be trying to gain access to your passwords or other sensitive information:
    - Do not click on links or attachments from untrusted sources, as they may contain malicious viruses or software.
    - Before responding to or taking action in response to a communication demanding immediate action, verify with your employer or IT support to determine whether it is legitimate.

- If you become aware of a potential or actual breach of personal information or personal health information, notify the appropriate person with your employer immediately so that steps can be taken to address the situation and minimize the potential impact of the breach.

ACCESS AND PRIVACY DIVISION
DIVISION DE L'ACCÈS À L'INFORMATION ET DE LA PROTECTION DE LA VIE PRIVÉE
230-65 rue Regent St., Fredericton, NB E3B 7H8
☏ 506.453.5965/877.755.2811
🖷 506.453.5963
aip-aivp@gnb.ca
www.ombudnb-aip-aivp.ca